

EXHIBIT 222

Automotive News

Dealers want secure connections

Computer system providers are reining in third-party vendors

Ralph Kisiel

Automotive News | June 12, 2006 - 12:01 am EST

A dealership group recently discovered that more than 100 third-party vendors had unauthorized access to its Reynolds and Reynolds Co. computer system.

Reynolds won't reveal which dealership group was the target, but the unauthorized access is not surprising. Dealerships often allow third-party vendors, such as lead generators and software providers, access to their computer systems to transmit and extract data.

These connections are commonly called hostile or unsupported interfaces because Reynolds -- or any other major supplier of dealership management systems -- is typically left out of the deals with third-party vendors.

Dealerships give third-party vendors access to their computer systems to extract inventory, service history and certain customer information. The vendors generally are providing services that the dealerships want and value.

But hundreds of third-party vendors sell software and services to dealerships. Problems arise when dealerships lose track of which vendors they have granted access to their computer systems. Some vendors have continued to extract information from dealership computer systems long after contracts have expired.

And the very nature of the hostile interface can cause big headaches for dealerships. Vendors that tap dealership systems through hostile interfaces are not always familiar with the systems. That has caused dealership systems to slow down, lock up and corrupt data.

"These are not necessarily isolated cases," says Clif Mason, vice president of product marketing for ADP Dealer Services.

Reynolds, ADP and Universal Computer Systems Inc., three of the largest suppliers of dealership management systems, offer third-party vendors alternatives to hostile interfaces. In the process, they are providing dealerships with data security and some peace of mind.

Reynolds, for example, has developed certified interfaces with J.D. Power and Associates' Power Information Network, Enterprise Rent-A-Car Co. and Stronghold Technologies Inc., to name a few.

ADP certification

Here is how ADP certifies a 3rd-party vendor.

- Vendor trains on ADP's dealership management system.
- ADP gives vendor software development kit.
- ADP helps vendor develop interface.
- Vendor tests interface.
- ADP monitors installation of interface.

Source: ADP Dealer Services

140 and counting

Universal, of Houston, has achieved some success at getting third-party vendors to use its formal Business Connexion

program. Universal now has 140 third parties using Universal-supported interfaces to exchange data with dealerships.

Universal contracts with a third-party vendor to jointly develop an interface between a dealership with a Universal system and the vendor.

The vendor benefits by having an interface designed specifically for exchange of data between its system and the dealership's system. The dealership benefits by restricting access to just the data that the vendor requires to provide the service.

Universal's Business Connexion customers include companies that offer data-based advertising, electronic title registration, F&I data transfers, Internet lead handling and vehicle inventory data transfers. Universal began the program in 2000.

"It's designed to protect the dealership system so that we know who's getting in, how they are getting in and what information they are getting their hands on," says Steve Henning, Universal's marketing manager. "Integration is the key. We know it works. It works consistently. It protects the dealers."

ADP, of Hoffman Estates, Ill., won't reveal how many authorized interfaces it has developed with third-party vendors but says dealerships are becoming more concerned about security of their data and are beginning to pressure third-party vendors to get a certified connection from ADP, Reynolds or Universal.

System shutdowns

Secure access is one of the tenets of ADP's vendor program, Mason says. "We've spent an inordinate amount of support and diagnosis time where a dealer system has gone down, been put out of commission, from a hostile interface," he says.

"Once ADP helps a third-party vendor to develop a certified interface with its system, that vendor only gets a level of access to a dealership's data that they require for their application," says Beth Ayotte, ADP's director of strategic alliances.

Third-party vendors benefit from certified interfaces as well, she says. For example, when ADP makes changes to its system, such as updating or adding new software, third-party vendors with a certified ADP interface will not have any disruption in their service to the dealerships, Ayotte says. Those vendors with hostile interfaces must scramble and figure out what changes ADP made to its system, she says.

ADP lists vendors on its Web site that have been certified under this program, including Rome Technologies, Graco Inc. and ProQuest Co.

Reynolds, of Dayton, Ohio, has 26 third-party vendors in its Reynolds Certified Interface program and another nine vendors under contract going through the certification process. The program was launched in 2003.

Building a brand

Richard Ward, Reynolds director of information services strategy, says he expects dealerships with the Reynolds system increasingly to ask third-party vendors whether they have this certification.

Dealerships have scores of hostile interfaces with third-party vendors because Reynolds and other system suppliers historically did not provide certification programs, Ward says.

He concludes: "The expectations and the needs for us to do things

in a safe, secure manner have increased dramatically in the past few years."

You may e-mail Ralph Kiesel at rkiesel@crain.com

PRINTED FROM: [http://www.autonews.com/apps/pbcs.dll/article?](http://www.autonews.com/apps/pbcs.dll/article?AID=/20060612/SUB/60609033&AssignSessionID=17333458_2457740&template=printart)
AID=/20060612/SUB/60609033&AssignSessionID=17333458_2457740&template=printart

Entire contents ©2009 Crain Communications, Inc.
